WHAT IS CLAIMED IS:

1. A host device for inputting/outputting data to/from a storage device for storing data, the host device comprising:

a controller which divides a series of cryptographic input/output processing for encrypting data to be secured and inputting/outputting the same into a plurality of procedures, and issues to the storage device a command for making the storage device execute a procedure to be executed on the storage-device side out of the procedures, and wherein

the controller obtains information for estimating time necessary to execute the command from the storage device prior to the issuance of the command, sets a wait time for the command based on the obtained information, issues the command to the storage device, and waits the time set for the command before it issues a command for the next procedure to the storage device.

2. The host device according to claim 1, wherein

the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary to execute the command.

3. The host device according to claim 1, wherein

the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary for at least one basic process out of an encrypting operation, a decrypting operation, a hash operation, a random number generating operation, and log retrieval which are used to execute the command.

4. A storage device comprising:

a storage medium which stores data;

a controller which receives a command from a host device in executing a series of cryptographic input/output processing for encrypting data to be secured and inputting/outputting the same between the storage medium and the host device, the command being issued as a result of division of the cryptographic input/output processing into a plurality of procedures; and

a cryptographic processing unit which executes the command, wherein

in response to a request from the host device, the controller provides information from which the host device estimates the time necessary for the cryptographic processing unit to execute the command.

5. The storage device according to claim 4, wherein

according to the processing procedures, the cryptographic input/output processing is divided into any of process units including:

a process for receiving data input from the host device and performing encryption or decryption using the cryptographic processing unit if necessary;

a process for performing encryption, decryption, or signature attachment using the cryptographic processing unit in order to output data to the host device; and

a process for outputting data to the host device, and

the command is issued by each of the process units divided.

6. The storage device according to claim 4, wherein

the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary to execute the command.

7. The storage device according to claim 5, wherein

the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary to execute the command.

8. The storage device according to claim 4, wherein

the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary for at least one basic process out of an encrypting operation, a decrypting operation, a hash operation, a random number generating operation, and log retrieval which are used to execute the command.

9. The storage device according to claim 5, wherein

the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary for at least one basic process out of an encrypting operation, a decrypting operation, a hash operation, a random number generating operation, and log retrieval which are used to execute the command.

10. The storage device according to claim 4, wherein

the controller checks if the commands issued as a result of division of the plurality of procedures are in regular order of execution.

11. The storage device according to claim 5, wherein

the controller checks if the commands issued as a result of division of the plurality of procedures are in regular order of execution.

12. A data input/output method for executing a series of cryptographic input/output processing for encrypting data to be secured and inputting/outputting the data between a

storage device for storing data and a host device, comprising:

dividing the cryptographic input/output processing into a plurality of procedures, and making the host device execute a procedure to be executed on the host-device side out of the procedures;

allowing the host device to issue a command to the storage device in order to make the storage device execute a procedure to be executed on the storage-device side;

allowing the storage device to receive the command; and

allowing the storage device to execute the command, wherein

the host device obtains information for estimating time necessary for the storage device to execute the command from the storage device prior to the issuance of the command, issues the command to the storage device, and waits the time estimated necessary to execute the command before it issues a command for the next procedure to the storage device.

13. The data input/output method according to claim 12, wherein

according to the processing procedures, the cryptographic input/output processing is divided into any of process units including:

a process for receiving data input from the host device and performing encryption or decryption using the cryptographic processing unit if necessary;

a process for performing encryption, decryption, or signature attachment using the cryptographic processing unit in order to output data to the host device; and

a process for outputting data to the host device, and

the command is issued by each of the process units divided.

14. The data input/output method according to claim 12, wherein

the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary to execute the command.

15. The data input/output method according to claim 13, wherein

the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary to execute the command.

16. The data input/output method according to claim 12, wherein

the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary for at least one basic process out of an encrypting operation, a decrypting operation, a hash operation, a random number generating operation, and log retrieval which are used to execute the command.

17. The data input/output method according to claim 13, wherein

the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary for at least one basic process out of an encrypting operation, a decrypting operation, a hash operation, a random number generating operation, and log retrieval which are used to execute the command.